AMENDMENTS TO THE CLAIMS

1. (Currently Amended) A method for applying a quality of service to an encrypted packet comprising:

during initial establishment of a secure control channel, receiving and storing an identifier associated with the quality of service in association with a first Internet Key Exchange (IKE) ID;

examining an encrypted packet;

without decrypting the encrypted packet, ~~determining whether~~ mapping a second IKE ID from the packet, using the first IKE ID, to the identifier associated with the quality of service ~~is present~~ in a profile portion of the encrypted packet;

in response to ~~determining that the identifier is present in the encrypted packet~~ mapping to the identifier associated with the quality of service, applying the associated quality of service to the encrypted packet.

2. (Currently Amended) The method of claim 1, further comprising the steps of:

before the examining:

encrypting the packet, wherein said step of encryption includes establishing ~~said identifier~~ the second IKE ID in the packet.

3. (Canceled)

4. (Currently Amended) The method of claim [[~~3~~]] 1, wherein the ~~Internet Key Exchange (IKE)~~ IKE ID comprises one or more of ID_IPV4_ADDR, ID_FQDN, ID_USER_FQDN, ID_IPV4_ADDR_SUBNET, ID_IPV6_ADDR, ID_IPV6_ADDR_SUBNET, ID_IPV4_ADDR_RANGE, ID_IPV6_ADDR_RANGE, ID_DER_ASN1_DN, ID_DER_ASN1_GN, and ID_KEY_ID.

5. (Currently Amended) The method of claim 1, wherein the identifier associated with the quality of service is based on at least an entry in a security association database.

6. (Currently Amended) The method of claim 1, wherein said identifier associated with the quality of service maps to a quality of service (QoS) group.

7. (Currently Amended) The method of claim 2, wherein the ~~identifier~~ first IKE ID is ~~established~~ created in a profile of the packet.

8. (Original) The method of claim 7, wherein the profile is an ISAKMP profile.

9. (Original) The method of claim 2, further comprising a step of pre-classification of the packet prior to the step of encryption.

10. (Currently Amended) The method of claim 9, wherein the quality of service that is applied is selected based on both the ~~identifier~~ second IKE ID and pre-classification.

11. (Currently Amended) A method for applying a quality of service to a packet comprising:

during initial establishment of a secure control channel, receiving and storing an identifier associated with the quality of service in association with a first Internet Key Exchange (IKE) ID;

encrypting the packet to create an encrypted packet;

examining an identifier in a profile portion of the encrypted packet, wherein the identifier is based on [[~~an~~]] a second IKE ID of the encrypted packet;

without decrypting the encrypted packet, ~~determining whether~~ mapping the second IKE ID from the packet, using the first IKE ID, to the identifier in the encrypted packet [[~~is~~]] associated with a quality of service to be applied to the encrypted packet; and

in response to ~~determining that the identifier is associated with a quality of service to be applied to the encrypted packet~~ mapping to the identifier associated with the quality of service, applying the quality of service to the encrypted packet.

12. (Currently Amended) The method of claim 11, further comprising the step of:

prior to the step of encrypting, pre-classifying the packet based on the contents of the packet;

wherein the quality of service that is applied to the packet is selected partially based the step of pre-classification and partially based on the ~~identifier~~ second IKE ID.

13. (Currently Amended) The method of claim 11, further comprising the step of:

during encryption, copying at least one bit into a header to identify a characteristic of the packet;

wherein the quality of service that is applied to the packet is selected partially based on a value of the at least one bit and partially based on the ~~identifier~~ second IKE ID.

14. (Currently Amended) A computer-readable volatile or non-volatile storage medium comprising one or more sequences of instructions, which when executed by one or more processors, cause the one or more processors to perform applying a quality of service to an encrypted packet by:

during initial establishment of a secure control channel, receiving and storing an identifier associated with the quality of service in association with a first Internet Key Exchange (IKE) ID;

examining an encrypted packet;

without decrypting the encrypted packet, ~~determining whether~~ mapping a second IKE ID from the packet, using the first IKE ID, to the identifier associated with the quality of service ~~is present~~ in a profile portion of the encrypted packet;

in response to ~~determining that the identifier is present in the encrypted packet~~ mapping to the identifier associated with the quality of service, applying the associated quality of service to the encrypted packet.

15. (Currently Amended) The computer-readable medium of claim 14 comprising one or more sequences of instructions, which when executed by one or more processors, cause the one or more processors to carry out before the examining:

encrypting the packet, wherein said step of encryption includes establishing ~~said identifier~~ the second IKE ID in the packet.

16. (Canceled)

17. (Currently Amended) The computer-readable medium of claim 14 wherein the ~~Internet Key Exchange (IKE)~~ IKE ID comprises one or more of ID_IPV4_ADDR, ID_FQDN, ID_USER_FQDN, ID_IPV4_ADDR_SUBNET, ID_IPV6_ADDR, ID_IPV6_ADDR_SUBNET, ID_IPV4_ADDR_RANGE, ID_IPV6_ADDR_RANGE, ID_DER_ASN1_DN, ID_DER_ASN1_GN, and ID_KEY_ID.

18. (Currently Amended) The computer-readable medium of claim 14 wherein the identifier associated with the quality of service is based on at least an entry in a security association database.

19. (Currently Amended) The computer-readable medium of claim 14 wherein said identifier associated with the quality of service maps to a quality of service (QoS) group.

20. (Currently Amended) The computer-readable medium of claim 15 wherein the ~~identifier~~ first IKE ID is ~~established~~ created in a profile of the packet.

21. (Previously presented) The computer-readable medium of claim 20 wherein the profile is an ISAKMP profile.

22. (Previously presented) The computer-readable medium of claim 15 further comprising one or more sequences of instructions, which when executed by one or more processors, cause the one or more processors to carry out pre-classification of the packet prior to the encryption.

23. (Currently Amended) The computer-readable medium of claim 22 wherein the quality of service that is applied is selected based on both the ~~identifier~~ second IKE ID and pre-classification.

24.-26. (Canceled)

27. (Currently Amended) An apparatus for applying a quality of service to an encrypted packet comprising:

means for receiving and storing an identifier associated with the quality of service in association with a first Internet Key Exchange (IKE) ID during initial establishment of a secure control channel;

means for examining an encrypted packet;

means for ~~determining~~ mapping, without decrypting the encrypted packet, ~~whether~~ a second IKE ID from the packet, using the first IKE ID, to the identifier associated with the quality of service ~~is present~~ in a profile portion of the encrypted packet;

means, responsive to the ~~determining~~ mapping means, for applying the quality of service to the encrypted packet ~~if it is determined that the identifier is present in the encrypted packet~~.

28. (Currently Amended) The apparatus of claim 27, further comprising means, operable before the examining means, for encrypting the packet, wherein the means for encryption includes means for establishing ~~said identifier~~ the second IKE ID in the packet.

29. (Canceled)

30. (Currently Amended) The apparatus of claim 29, wherein the ~~Internet Key Exchange (IKE)~~ IKE ID comprises one or more of ID_IPV4_ADDR, ID_FQDN, ID_USER_FQDN, ID_IPV4_ADDR_SUBNET, ID_IPV6_ADDR, ID_IPV6_ADDR_SUBNET, ID_IPV4_ADDR_RANGE, ID_IPV6_ADDR_RANGE, ID_DER_ASN1_DN, ID_DER_ASN1_GN, and ID_KEY_ID.

31. (Currently Amended) The apparatus of claim 27, wherein the identifier associated with the quality of service is based on at least an entry in a security association database.

32. (Currently Amended) The apparatus of claim 27, wherein said identifier associated with the quality of service maps to a quality of service (QoS) group.

33.-36. (Canceled)

37. (Currently Amended) An apparatus for applying a quality of service to an encrypted packet comprising:

one or more processors;

memory communicatively coupled to the one or more processors;

one or more sequences of instructions in the memory for applying a quality of service to an encrypted packet, which instructions, when executed by the one or more processors, cause the one or more processors to perform the steps of:

during initial establishment of a secure control channel, receiving and storing an identifier associated with the quality of service in association with a first Internet Key exchange (IKE) ID;

examining an encrypted packet;

without decrypting the encrypted packet, ~~determining whether~~ mapping a second IKE ID from the packet, using the first IKE ID, to the identifier associated with the quality of service ~~is present~~ in a profile portion of the encrypted packet;

in response to ~~determining that the identifier is present in the encrypted packet~~ mapping to the identifier associated with the quality of service, applying the quality of service to the encrypted packet.

38. (Currently Amended) The apparatus of claim 37, further comprising sequences of instructions for performing the steps of:

before the examining:

encrypting the packet, wherein said step of encryption includes establishing said ~~identifier~~ the second IKE ID in the packet.

39. (Canceled)

40. (Currently Amended) The apparatus of claim 39, wherein the ~~Internet Key Exchange (IKE)~~ IKE ID comprises one or more of ID_IPV4_ADDR, ID_FQDN, ID_USER_FQDN, ID_IPV4_ADDR_SUBNET, ID_IPV6_ADDR, ID_IPV6_ADDR_SUBNET, ID_IPV4_ADDR_RANGE, ID_IPV6_ADDR_RANGE, ID_DER_ASN1_DN, ID_DER_ASN1_GN, and ID_KEY_ID.

41. (Currently Amended) The apparatus of claim 37, wherein the identifier associated with the quality of service is based on at least an entry in a security association database.

42. (Currently Amended) The apparatus of claim 37, wherein said identifier associated with the quality of service maps to a quality of service (QoS) group.

43. (Currently Amended) The apparatus of claim 38, wherein the ~~identifier~~ first IKE ID is ~~established~~ created in a profile of the packet.

44. (Original) The apparatus of claim 43, wherein the profile is an ISAKMP profile.

45. (Original) The apparatus of claim 38, further comprising a step of pre-classification of the packet prior to the step of encryption.

46. (Currently Amended) The apparatus of claim 45, wherein the quality of service that is applied is selected based on both the ~~identifier~~ second IKE ID and pre-classification.

47. (Currently Amended) The apparatus of claim 28, wherein the ~~identifier~~ first IKE ID is ~~established~~ created in a profile of the packet.

48. (Previously presented) The apparatus of claim 33, wherein the profile is an ISAKMP profile.

49. (Previously presented) The apparatus of claim 28, further comprising means for pre-classification of the packet prior to the step of encryption.

50. (Currently Amended) The apparatus of claim 35, comprising means for selecting the quality of service that is applied based on both the ~~identifier~~ second IKE ID and pre-classification.